

RECEIVED  
CENTRAL FAX CENTER  
JUL 05 2007



## FACSIMILE COVER SHEET

July 5, 2007

**Receiver:** Examiner Jalatee Worjlloh  
Appeal Briefs - Patents

**FAX #:** 571-273-8300

**Sender:** Rupak Nag

**Application No:** 09/842,313

**Re:** Appeal Brief  
Our File No.: VISAP064

**Pages Including Cover Sheet(s):** 24

### MESSAGE:

**Please see attached.**

Appeal Brief Transmittal  
Appeal Brief

2 pages  
21 pages

---

### CONFIDENTIALITY NOTE

The information contained in this facsimile (FAX) message is legally privileged and confidential information intended only for the use of the receiver or firm named above. If the reader of this message is not the intended receiver, you are hereby notified that any dissemination, distribution or copying of this FAX is strictly prohibited. If you have received this FAX in error, please immediately notify the sender at the telephone number provided below and return the original message to the sender at the address below via the United States Postal Service. Thank you.

---

Beyer Weaver LLP • 500 15th Street, Suite 200, Oakland, CA 94607 • Phone 510.663.1100 • Fax 510.663.0930 • [www.beyerlaw.com](http://www.beyerlaw.com)  
Cupertino • Minneapolis • Oakland

RECEIVED  
CENTRAL FAX CENTER

JUL 05 2007

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Weller et al.

Attorney Docket No.: VISAP064

Application No.: 09/842,313

Examiner: WORJLOH, Jalatee

Filed: April 24, 2001

Group: 3621

Title: ONLINE PAPER AUTHENTICATION  
SERVICE

## CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted to the U.S.  
Patent and Trademark Office, Central Facsimile Telephone number  
(571) 273-8300 on this day July 5, 2007, addressed to Examiner Jalatee  
Worjloh.

Signed: \_\_\_\_\_

Rupak Nag

**APPEAL BRIEF TRANSMITTAL  
(37 CFR 192)**

Mail Stop Appeal Brief-Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the Notice of Appeal filed in this case on January 4, 2007.

This application is on behalf of

☐ Small Entity☒ Large Entity

Pursuant to 37 CFR 1.17(f), the fee for filing the Appeal Brief is:

☐ \$250.00 (Small Entity) ☒ \$500.00 (Large Entity)

☐ Applicant(s) hereby petition for a \_\_\_\_\_ extension(s) of time to under 37 CFR 1.136.

If an additional extension of time is required, please consider this a petition therefor.

☐ An extension for \_\_\_\_\_ months has already been secured and the fee paid therefor of  
\$ \_\_\_\_\_ is deducted from the total fee due for the total months of extension now requested.

☒ Applicant(s) believe that no Extension of Time is required; however, if it is  
determined that such an extension is required, Applicant(s) hereby petition that such an extension

07/06/2007 TL0111 00000031 500388 09842313

01 FC:1402

500.00 DA

PAGE 03/24  
**RECEIVED**  
CENTRAL FAX CENTER  
JUL 05 2007

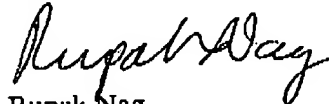
be granted and authorize the Commissioner to charge the required fees for an Extension of Time under 37 CFR 1.136 to Deposit Account No. 500388.

|                        |       |
|------------------------|-------|
| Total Fee Due:         |       |
| Appeal Brief fee       | \$500 |
| Extension Fee (if any) | NA    |
| Total Fee Due          | \$500 |

☐ Enclosed is Check No. in the amount of \$ .

☒ Charge any additional fees or credit any overpayment to Deposit Account No. 500388, (Order No. VISAP064).

Respectfully submitted,  
BEYER WEAVER LLP

  
Rupak Nag  
Reg. No. 37,493

P.O. Box 70250  
Oakland, CA 94612-0250  
(612) 252-3335

**RECEIVED**  
**CENTRAL FAX CENTER**

**JUL 05 2007**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**  
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

---

**EX PARTE Weller et al.**

---

**Application for Patent**

**Filed: April 24, 2001**

**Application No. 09/842,313**

**FOR:**

**ONLINE PAYER AUTHENTICATION SERVICE**

---

**APPEAL BRIEF**

---

**CERTIFICATE OF FACSIMILE TRANSMISSION**

I hereby certify that this correspondence is being transmitted to the U.S. Patent and Trademark Office, Central Facsimile Telephone number (571) 273-8300 on this day July 5, 2007 addressed to Examiner J. J. Worjloh

Signed: \_\_\_\_\_

Rupak Nag

**BEYER WEAVER LLP**  
**Attorneys for Appellants**

Attorney Docket No. VISAP064

-i-

Application No. 09/842,313

**RECEIVED**  
**CENTRAL FAX CENTER****JUL 05 2007****TABLE OF CONTENTS**

|   | <u>Page No.</u> |
|---|-----------------|
| <b>I. REAL PARTY IN INTEREST</b>  | <b>1</b>        |
| <b>II. RELATED APPEALS AND INTERFERENCES</b>  | <b>1</b>        |
| <b>III. STATUS OF CLAIMS</b>  | <b>1</b>        |
| <b>IV. STATUS OF AMENDMENTS</b>   | <b>1</b>        |
| <b>V. SUMMARY OF CLAIMED SUBJECT MATTER</b>   | <b>1</b>        |
| <b>VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL</b>  | <b>4</b>        |
| <b>VII. ARGUMENT</b>  | <b>4</b>        |
| <b>A. The <i>Barnes</i> and <i>O'Mahony</i> References do not teach that the Account Issuer performs Card Owner Identity Authentication before and during an Online Transaction</b> | <b>4</b>        |
| <b>B. Conclusion</b>  | <b>11</b>       |
| <b>VIII. CLAIMS APPENDIX</b>  | <b>12</b>       |
| <b>IX. EVIDENCE APPENDIX</b>  | <b>17</b>       |
| <b>X. RELATED PROCEEDINGS APPENDIX</b>  | <b>18</b>       |

**I. REAL PARTY IN INTEREST**

The real party in interest is Visa International Service Association, 900 Metro Center Blvd., Foster City, CA 94308.

**II. RELATED APPEALS AND INTERFERENCES**

There are no related appeals or judicial proceedings known to the Appellants.

**III. STATUS OF CLAIMS**

|                     |                |
|---------------------|----------------|
| Allowed claims:     | None           |
| Claims objected to: | None           |
| Claims rejected:    | 7-21 and 32-40 |
| Claims on Appeal:   | 7-21 and 32-40 |

**IV. STATUS OF AMENDMENTS**

No amendments were filed following the Office Action of Oct. 4, 2006.

**V. SUMMARY OF CLAIMED SUBJECT MATTER**

The present invention is directed towards an online service for authenticating the identity of a person making a payment during an online transaction using, for example, a credit card or debit card. The invention is relatively easy to implement, requires minimal investment of resources, and provides a high level of interoperability between the purchaser's system (e.g., personal computer), the online merchant's system, and the system of the entity that issued the card being used by the purchaser. The purchaser authentication service of the present invention allows *a card issuer to verify a cardholder's identity* (the purchaser's identity) using a variety of authentication methods, such as the use of passwords. The only entity requiring a certificate is the entity, such as a financial institution, issuing the card to the purchaser. The authentication service of the

present invention can also provide authentication results to the online merchant in real time during the online checkout process. The authentication service of the present invention lays the foundation for establishing guaranteed payments for merchants involved with "card not present" transactions, such as online transactions. Additionally, the authentication service will reduce "chargebacks," frauds, and exception-item processing.

Claim 1 recites a method in which an account issuer authenticates, for the benefit of a third party, such as an online merchant, that a customer using an account during an online transaction with the third party is the actual owner of said account. The third party desires verification as to the identity of the customer before proceeding with the online transaction with the customer. The card issuer verifies during a card registration process the identity of the customer as the owner of the account and associating a designated password with the account. The card issuer requests that the customer enter the password during the online transaction. The card issuer verifies that the password entered by the customer is correct and matches the designated password established during the card registration process. The third party, such as the online merchant, is notified during the online transaction by the card issuer that the customer is the actual owner of said account when the passwords match. In this manner the card issuer authenticates the customer for the third party during the online transaction.

Claim 20 recites a method performed by a "payment authentication service" in which a card account issuer authenticates, for the benefit of a third party, such as an online merchant, that a customer using an account during an online transaction with the third party is the actual owner of the account. The card issuer verifies the customer's or new account holder's identity during a card registration process during which a password is associated with the new account. During an online transaction, an authentication request originates from a third-party software module and is sent via a customer computer to the access control server operated by the card issuer. The card issuer requests that the customer enter the password associated with the account which the card issuer then compares to the password associated with the account. The card issuer sends an authentication response message to the third-party software module containing an authentication status indicator which is used to authenticate the customer to the third party.

Claim 21 recites a method performed on a customer computer (for example, making an online purchase) in conjunction with a payment authentication service. In the process an issuing financial institution authenticates, for the benefit of a third party, that a

customer using a card account during an online transaction with the third party is the actual owner of said account. The customer sends enrollment information to card enrollment web site during a registration process so that a card issuer can verify the identity of the customer as the owner of the card account. The customer supplies a password to be designated with the account during the registration process. During an online transaction, the customer receives an authentication request message from the third party during an online transaction, the message requests initiation of a payment authentication service in which the identity of the customer will be authenticated. The authentication request message is sent to an access control server operated by a financial institution associated with the card issuer, the customer having an account with the financial institution. The customer receives a request from the access control server asking the customer to enter a password that will be used to verify the identity of the customer during the online transaction. The customer supplies the password which is used to verify the customer's identity. The customer computer facilitates sending an authentication response message from the access control server to the third party the response message regarding verification of the identity of the customer. In this manner the access control server verifies the identity of the customer for the third party.

Claim 32 recites a method performed by a payment authentication service in which an account issuer, such as a credit card issuer, authenticates a customer (e.g., credit card holder) for the benefit of a third party, such as an online merchant. The account issuer verifies during a registration process the identity of the customer as the owner of an account, such as a client, and associating a designated password with the account. The account issuer receives a request from a customer computer to perform a financial transaction with the third party and determines whether the customer is enrolled in the payment authentication service. The account issuer sends an authentication request message from the third party computer (e.g., online merchant system) over a network via the customer computer during the financial transaction, the authentication request message received at a computer under control of the account issuer. The third party receives an authentication response message from the computer of the account issuer via the customer computer during the financial transaction, the message indicating the authenticity of the customer. The authenticity is based upon a password supplied by the customer to the account issuer's computer during the financial transaction and upon the password previously designated for the account.



## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejection presented for review is as follows:

A. The rejection of claims 7-21 and 32-40 under 35 U.S.C. § 103 (a) as being unpatentable under U.S. Patent No. 5,970,475 issued to *Barnes et al.* in view of *O'Mahony*.

## VII. ARGUMENT

With respect to Ground A above, the rejected claims are argued as a single group.

### **A. The *Barnes* and *O'Mahony* References do not teach that the Account Issuer performs Card Owner Identity Authentication before and during an Online Transaction**

The Examiner has rejected claims 7-21 and 32-40 under §103 as being unpatentable over *Barnes et al.* in view of *O'Mahony*, "Electronic Payment Systems". As explained in the claims summary above, the present invention is a user identity authentication system that enables an online merchant, in one example, to ensure that a credit card number it receives during an online transaction with a customer belongs to that customer. This assurance is provided by the credit card issuer who verifies and establishes for future transactions the identity of the customer when the card is issued.

In the Office Action dated March 10, 2006, the Examiner agreed that *Barnes et al.* does not teach or suggest that an issuing party authenticates a user or customer during a transaction. Accordingly, subsequent Office Actions rely on *O'Mahony* to disclose payment systems where an issuer verifies consumers and authenticates financial transactions. Respectfully, it is submitted that the various payment schemes (especially First Virtual, CARI and CyberCash) disclosed in *O'Mahony* are distinguishable from the currently claimed invention.

Claims 7, 20, 21 and 32 recite that it is the issuer of the account, for example, credit card, debit card, check card accounts etc., that takes responsibility for verifying the identity of the customer as the owner of the account during an initial card registration process as recited in the first step of the claims. It is also the issuer that compares the password received from the customer during a transaction with the originally recorded password for that account established when the customer first obtained the card, as recited

in subsequent steps of the independent claims. The specification describes "issuer" at pages 8 and 9 of the specification. Thus, the issuer verifies the identity of the new cardholder when an account is established and performs the customer identity verification and authentication service for a third party after the card has been issued and is being used.

Because the card issuer is the entity that establishes and maintains the user's account, there are advantages in having the issuer enroll the user in the authentication system of the invention. The issuer already holds a wealth of information about the customer (obtained during the enrollment or registration process) and can use this information to verify the identity of the customer much better than nearly any other entity given that other entities may not have a prior relationship with the customer. For example, the issuer has a cardholder system 110 that includes account information and services utilized by a cardholder. An identity authentication database 116 contains information that the issuer already has on file regarding a cardholder (e.g., an online customer) and is used by the issuer to enroll cardholders and to verify their identities. See for example pages 9-10 of the specification. Consequently, an issuer can provide identity authentication policies and other information that an online merchant can use in an identity verification process during an online transaction.

The issuer is able to use the above information it already holds to verify the identity of a prospective user or customer during registration and to provide a solid assurance that the password associated with that account is being provided by the person that the prospective customer claims to be. An organization other than the credit card account issuer (or debit card issuer) does not always have access to this information and cannot guarantee to the same level that the person to whom the password is issued is the person they claim to be. The systems described in *O'Mahony* (especially First Virtual, CARI and CyberCash) are deficient in that they do not teach or suggest that the issuer of the user account is the organization that registers the user and compares the passwords during a subsequent transaction, thereby verifying the identity of the user.

#### First Virtual

Figure 4.2 at page 66 of *O'Mahony* illustrates the First Virtual authentication system. A buyer (analogous to an entity or user) is buying goods from a merchant (analogous to a third party); a First Virtual server authenticates the buyer's identifier for the merchant. (The identifier is a so-called "VirtualPIN" or password.) First Virtual does not issue a credit card to the buyer and does not issue an account to the buyer that the

buyer is attempting to authenticate; it simply is not an issuer. First Virtual is an unrelated company that performs the service of authentication for the buyer and merchant. In fact, a credit card company views First Virtual as a merchant, not as an issuer (third to last paragraph).

Because First Virtual is not an issuer it performs virtually no verification of the buyer's identity when the buyer registers. A buyer registers with First Virtual by forwarding his credit card details and in return receiving a password (third paragraph). There is no verification of the buyer's identity being performed before the buyer can receive a valid password from First Virtual. By contrast, independent claims 7, 20, 21 and 32 require that the issuer verify the identity of the entity as the owner of the account during registration or enrollment. Because First Virtual does not verify the buyer's identity during registration (as is required by the independent claims), the authentication system of First Virtual cannot guarantee the identity of the buyer. For example, the article states "the system is not entirely fraudproof" (first paragraph) and that "bogus purchases can be made from then until such time as the VirtualPIN is blacklisted (fifth paragraph from the end). Further, "a stolen credit card number could be used to set up VirtualPINs associated with e-mail addresses controlled by the attacker" (fourth paragraph from the end).

Stolen credit card numbers can be used to set up fake passwords because there is no verification of the buyer's identity during registration (because First Virtual does not have access to an issuer's user account information). The inventions of claims 7, 20, 21 and 32 nearly guarantee that stolen numbers cannot be used to set up fake passwords because the issuer verifies the user's identity during registration. Further, it is First Virtual that compares the passwords at the request of the merchant (fifth paragraph); it is not the issuer of the credit card account that does the comparison as is required by the independent claims.

### CARI

Figure 4.4 at page 69 and figure 4.5 at page 71 of *O'Mahony* illustrate registration and purchase using the CARI authentication system. A consumer (analogous to an entity or user) is buying goods from a merchant (analogous to a third party); a CARI machine authenticates the consumer's virtual credit card number for the merchant. (The virtual credit card number or "VCC" is a random number assigned by CARI; we refer to it as a password.) CARI does not issue a credit card to the consumer and does not issue an account to the consumer that the consumer is attempting to authenticate; CARI simply is

not an issuer. CARI is an unrelated company that performs the service of authentication for the consumer and merchant.

Because CARI is not an issuer it performs virtually no verification of the consumer's identity when the consumer registers. To register (section 4.4.2), a user enters personal details such as name, e-mail address, shipping address and telephone number, and then provides credit card details to CARI by telephone. The user is then assigned a password which is then activated. But, there is no verification of the user's identity being performed by the account issuer before the user can receive a valid password from CARI. By contrast, independent claims 7, 20, 21 and 32 require that the issuer verify the identity of the entity as the owner of the account during registration or enrollment. At the end of section 4.4.2 it is stated that "the real card is verified" but presumably this can only mean checking the name on the credit card with the name previously provided. CARI cannot perform extensive verification of the user's identity because it does not have access to the wealth of information that an account issuer has.

A stolen credit card can be used to set up a fake user in the CARI system because there is no verification of the user's identity during registration by an issuer (because CARI is not an issuer and does not have access to a credit card issuer's account information). A thief can steal a card and then supply the appropriate personal details using the name on the card. Because CARI is not an issuer and cannot verify the user's identity during registration (as is required by the independent claims), the authentication system of CARI cannot guarantee the identity of the user. The inventions of claims 7, 20, 21 and 32 nearly guarantee that stolen numbers cannot be used to set up fake users because the issuer verifies the user's identity during registration. Further, it is CARI that compares the passwords at the request of the merchant (section 4.4.4); it is not the issuer of the credit card account that does the comparison as is required by the independent claims.

Further, claim 7 requires that the issuer receive from the customer during the online transaction an identity authenticating password, and that the issuer notify "said third party over said network during said online transaction." CARI discloses an NFS client (that compares the passwords) that is not on line and does not communicate with the consumer. Claim 20 requires that the issuer request and verify a password from the customer; claim 21 requires that the customer receives a request from an access control server of the issuer to enter a password; and claim 32 requires that the customer supply a password to a computer of the issuer during a financial transaction. CARI does not

disclose that the consumer communicates directly with CARL. Further, CARL cannot authenticate a user to a merchant on line and in real time because it sends order information "to the merchant via fax, secure ftp, encrypted e-mail, or a dial-up line." Even if FTP, e-mail or a dial-up line is used, authentication cannot happen in real time because a connection to the merchant must be established; there is no existing online connection such as would exist in the case of an Internet connection.

#### CyberCash

The CyberCash system described in section 4.6 likewise does not disclose an account issuer that verifies the identity of the customer during a registration process and obtains a password. Relevant parts of the CyberCash system are shown in Figures 4.10 and 4.11. As described, CyberCash does not rely upon a customer registration process to establish the identity of the customer and to associate a password with that account. By contrast, CyberCash relies upon digital signatures. In fact, as described in the first two paragraphs of section 4.6.3, it would be possible for an unscrupulous party to simply sit down at a legitimate customer's computer and engage in a financial transaction because no password is required of the user in order to engage in a transaction. The customer's credit card is registered with the software previously, but such a process does not include verifying the customer's identity as the owner of a financial account.

Therefore, the CyberCash system does not teach or suggest verifying the identity of a customer as the owner of an account during a registration process, but rather teaches a more complex scheme relying upon digital signatures.

#### The Remaining Payment Systems in *O'Mahony*

None of the other remaining payment systems described in the other sections of Chapter 4 teach or suggest that the issuer of an account verifies during a registration process the identity of the customer as the owner of the account. Section 4.5 discusses SSL that does not involve an account issuer as a trusted party. The iKP system of section 4.7 relies upon public-key cryptography; section 4.8 is based upon the 3KP technique of section 4.7. The SET system of section 4.9 is also based upon public-key cryptography. The electronic check systems of Chapter 5 all involve electronic checks and likewise do not disclose an issuer verifying the identity of the customer during a registration process.

The Final Office Action and the *Barnes* Reference

Page 2 of the Final Office Action mailed October 4, 2006 points out that *Barnes* discloses in Figure 5 and in the associated text a procurement system that handles the registration process and subsequent authentication procedures.

Independent claims 7, 20, 21 and 32 each require three different entities: a customer, a third-party (such as a merchant) and an account issuer (e.g., credit card issuer, debit card issuer, etc.). The issuer authenticates the customer for the benefit of the third party during an online transaction so that the merchant, for example, is certain that the credit card he is receiving during an online purchase is coming from the person who "owns" that credit card account and not someone else, such as someone who stole the credit card, an online imposter, or even a friend or family member who may have access to the card but does not have permission or authorization to use it.

Respectfully, it is pointed out that *Barnes* does not involve an additional trusted party for the purposes of authentication during a transaction. Figure 5 of *Barnes* shows a customer 24 executing a purchase transaction with a supplier system 16 or seller; there is no trusted party involved during the transaction because the two parties authenticate one another using well-known public-key cryptography techniques.

There is no disclosure that the identity of a user is verified, nor that an outside party (such as an account issuer) is performing the verification. The bank ACH security software as described in column 15 of *Barnes* does not enable the bank to perform the customer identity verification during a transaction between a third party, such as an online merchant, and a customer. In any case, Figure 5 only shows two parties interacting. All of the independent claims require three entities interacting, including a trusted account issuer that verifies the identity of the customer. Figure 5 might disclose a purchaser being authorized by a procurement system, but this authorization is being performed by the purchaser's own company; i.e., the purchaser is an employee of the buying organization 12.

Claims 7, 20, 21 and 32 specifically require that it is the issuer of the account that takes responsibility for verifying the identity of the customer as the owner of the account during a registration process. It is also the issuer that compares the password received from the customer with the originally recorded password for that account during the online transaction between the customer and the third-party merchant. *Barnes* does not disclose

in any manner that there is a third entity namely, an issuer, which verifies the identity of the customer during a separate registration process.

For one, *Barnes* does not disclose any third entity such as an issuer that verifies the identity of the customer; *Barnes* only discloses that it is the customer's organization itself that might authorize the customer. Secondly, there is no true verification of the customer's identity occurring during an online transaction. *Barnes* uses the word "authenticated" in column 8, but there is no disclosure suggesting that the identity of the customer is actually verified. Thirdly, as required by the independent claims, there is no third entity that not only performs verification of identity during a registration process, but also authenticates that same customer during an online transaction.

#### Dependent Claims

Claim 9 requires determining if a user is enrolled by looking at a database of enrolled accounts; the cited art does not disclose checking to see if a user is enrolled before performing the authentication process. Claim 14 requires that the issuer or an access control server of the issuer sign a transaction receipt using a signature key; again, the cited art does not disclose that it is the issuer that authenticates a user and thus is able to provide a signed transaction receipt.

Dependent claims 37-40 all require that the authentication request from the third party to the issuer is routed via a computer of the user. Such features are not taught or suggested in the art of record. The advantage of these features is that as long as the user's computer has connected to a merchant computer over an online connection, it is convenient for the merchant computer to query the issuer computer via the user's browser. The issuer computer is then conveniently connected to the user computer and can ask for the identity-authenticating password.

Dependent claim 10 requires that it is determined whether the user is registered or enrolled before sending a request from the third party to the issuer for authentication. Such features are not taught or suggested in the art of record. Depending upon the embodiment, the specification discloses that this determination can occur by checking a directory server (or other database) to see if a user's account number is present in a list of enrolled users, or by checking to see if the user computer has special software installed. The advantage of these features is that a quick check for an enrolled user can avoid a time-consuming and error-prone authentication process for users that are not enrolled.

RECEIVED  
CENTRAL FAX CENTER

JUL 05 2007

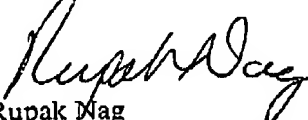
**B. Conclusion**

In view of the foregoing, all of the claim rejections under 35 U.S.C. § 103 (a) as being unpatentable by *Barnes et al.* in view of *O'Mahony* cannot stand for at least the reasons discussed.

In view of the foregoing, Appellants respectfully request that the Board reverse the Examiner's rejection of all pending claims. In addition, Appellants believe all claims now pending in this application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

Respectfully Submitted,

BEYER WEAVER LLP

Rupak Nag  
Registration No. 37,493BEYER WEAVER LLP  
P.O. Box 70250  
Oakland, CA 94612-0250  
Telephone: (612) 252-3335



**RECEIVED  
CENTRAL FAX CENTER****JUL 05 2007****VIII. CLAIMS APPENDIX****CLAIMS ON APPEAL**

7. A method wherein an account issuer authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said third party desiring verification as to the identity of said customer before proceeding with said online transaction with said customer, said method comprising:

verifying, by said issuer during a registration process, the identity of said customer as the owner of said account and associating a designated password with said account;

requesting over a network, by said issuer from said customer during said online transaction, of an identity-authenticating password;

verifying, by said issuer, that said identity-authenticating password from said customer matches said password previously designated for said account; and

notifying said third party over said network during said online transaction, by said issuer, that said customer is the actual owner of said account when said identity-authenticating password entered by said customer matches the password that was previously designated for said account, whereby said issuer authenticates said customer for said third party during said online transaction.

8. A method as recited in claim 7 wherein said issuer is an issuer financial institution and said third party is an online merchant, whereby said online merchant conducts an online financial transaction with said customer, and wherein said account of said customer is maintained by said issuer financial institution.

9. A method as recited in claim 7 further comprising:

querying an access control server to determine if an account of said customer is enrolled in a payment authentication service.

10. A method as recited in claim 9 wherein the access control server determines if said customer account is enrolled by verifying that said customer account is contained in a database of enrolled customer accounts.

11. A method as recited in claim 9 further comprising:  
querying a directory server to verify that said customer account is associated with an issuer financial institution that is participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.
12. A method as recited in claim 11 further comprising:  
sending to said third party's computer system an Internet address for said access control server, said Internet address passing through said directory server before reaching said third party's computer system, whereby said Internet address for said access control server allows said third party to directly communicate with said access control server.
13. A method as recited in claim 9 further comprising:  
reviewing a memory device controlled by said third party to verify that said customer account is associated with an issuer financial institution participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.
14. A method as recited in claim 7 further comprising:  
generating, by said issuer, a digitally-signed transaction receipt using a signature key of said trusted party; and  
sending, by said issuer, said digitally-signed transaction receipt to said third party, whereby said digitally-signed transaction receipt confirms to said third party that the identity of said customer has been authenticated.
15. A method as recited in claim 14 wherein said transaction receipt includes a number associated with said customer account, a transaction payment amount, and a transaction payment date.
16. A method as recited in claim 7 further comprising:  
sending, by said issuer, of a card authentication verification value to said third party, the card authentication verification value containing a unique value for said customer account and a specific payment transaction, whereby said card authentication

verification value uniquely identifies a specific authenticated payment transaction.

17. A method as recited in claim 14 further comprising:

verifying, by said third party, said digitally signed transaction receipt such that said third party is assured that said transaction receipt was sent from a specific issuer.

18. A method as recited in claim 7 further comprising:

sending, by said third party, of an authorization message to an issuer financial institution to verify said customer account has adequate credit for a requested purchase.

19. A method as recited in claim 7 wherein said customer enrolls in said payment authentication service in said registration process, said step of verifying further comprising:

receiving, by said trusted party, of enrollment information entered at an enrollment Internet web site by said customer;

verifying, by said trusted party, that said enrollment information substantially matches information contained within a pre-existing database of customer information; and

storing said customer account information in a database for enrolled customer accounts.

20. A method performed by a payment authentication service wherein an account issuer authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said method comprising:

verifying, by said issuer during a registration process, the identity of said customer as the owner of said account and associating a designated password with said account;

sending an authentication request message via a customer computer from a third-party software module over a network during said online transaction;

receiving said authentication request message at an access control server that is operated by said issuer;

requesting over said network, by said issuer, of a password from said customer;

verifying, by said issuer, that said password entered by said customer matches said password previously designated for said account; and

sending over said network, by said issuer, an authentication response message to a

third-party software module, said payment response message containing an authentication status indicator, whereby said issuer authenticates said customer for said third party.

21. A method performed by used with a payment authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said method comprising:

sending enrollment information to an enrollment web site by said customer during a registration process so that said issuer verifies the identity of said customer as the owner of said account;

supplying a password to be designated for said account during said registration process;

receiving an authentication request message from said third party during said online transaction that requests the initiation of a payment authentication service wherein the identity of said customer will be authenticated;

sending said authentication request message to an access control server operated by said issuer financial institution, said customer having an account with said issuer financial institution;

receiving a request from said access control server for said customer to enter a password used to verify the identity of said customer during said online transaction; and

supplying said password used to verify identity; and

facilitating the sending of an authentication response message from said access control server to said third party via said customer computer regarding the verification of the identity of said customer, whereby said access control server verifies the identity of said customer for said third party.

32. A method performed by a payment authentication service wherein an account issuer authenticates a customer for the benefit of a third party, said method comprising:

verifying, by said issuer during a registration process, the identity of said customer as the owner of said account and associating a designated password with said account;

receiving a request over a network from a customer computer to perform a financial transaction with said third party;

determining that said customer is enrolled in said payment authentication service;

sending an authentication request message from said third party via said customer computer over a network during said financial transaction, said authentication request message destined for a computer of said issuer;

receiving an authentication response message from said computer of said issuer via said customer computer during said financial transaction, said authentication response message indicating the authenticity of said customer, said authenticity being based upon a password supplied by said customer to said computer of said issuer during said financial transaction and upon said password previously designated for said account, whereby said issuer authenticates said customer for said third party.

33. A method as recited in claim 7 wherein said online transaction is a payment transaction.

34. A method as recited in claim 20 wherein said online transaction is a payment transaction.

35. A method as recited in claim 21 wherein said online transaction is a payment transaction.

36. A method as recited in claim 32 wherein said financial transaction is a payment transaction.

37. A method as recited in claim 20 wherein said payment authentication service uses a centralized architecture, and wherein said third-party software module sends said authentication request message to said access control server by way of a browser in said customer computer.

38. A method as recited in claim 20 wherein said payment authentication service uses a distributed architecture, wherein said third-party software module sends said authentication request message to a software module of said customer computer and wherein said customer computer then sends said authentication request message to said access control server.

39. A method as recited in claim 32 wherein said payment authentication service uses a centralized architecture, and wherein said third party sends said authentication request message to said issuer computer by way of a browser in said customer computer.

40. A method as recited in claim 32 wherein said payment authentication service uses a distributed architecture, wherein said third party sends said authentication request message to a software module of said customer computer and wherein said customer computer then sends said authentication request message to said issuer computer.

**RECEIVED  
CENTRAL FAX CENTER**

**JUL 05 2007**

**IX. EVIDENCE APPENDIX**

NONE

**RECEIVED  
CENTRAL FAX CENTER**

**JUL 05 2007**

**X. RELATED PROCEEDINGS APPENDIX**

NONE

**X. RELATED PROCEEDINGS APPENDIX**

Attorney Docket No. VISAP064

-18-

Application No. . 09/842,313

NONE